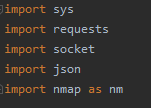
As we are using command line (CMD) to give the argument so that’s why we import sys library.

For banner grabber we will be using requests module and make GET requests to the server and then print the response that’s why we import requests library.

As we have to get the host name (with the help of built-in function of gethostbyname) and the hosts Ip address so that’s why we import the socket library.

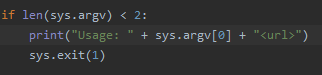
As we are getting the response of the request so to get response in json format we import the json library.

As we are scanning the ports with the help of nmap so that’s why we import nmap library.



As we provide Command line argument on cmd containing the address of the site we want to grab the banner for it so this is basically a check and display msg if there is no argument provided.

sys. Argv [0] is the name of the script like the main point is we write on CMD is ->python EHD.py "facebook.com"

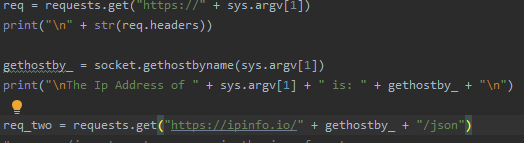
-

we are making GET request to HTTPS and then request the domain which we provide as argument(sys.argv[1]) in cmd

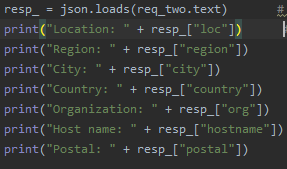
req variable will have the site

as we use socket module for use the function of the socket module gethostbyname and this function will get the ip address of the site

Then in req\_two we made the get request to API to get the response in json format

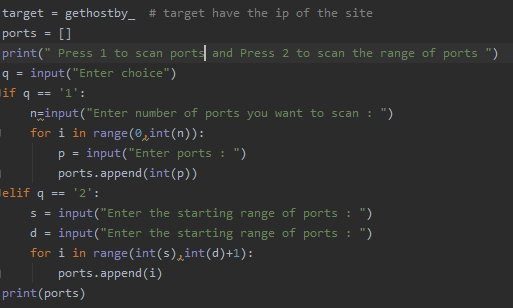


Here we got the response and important banners of the site

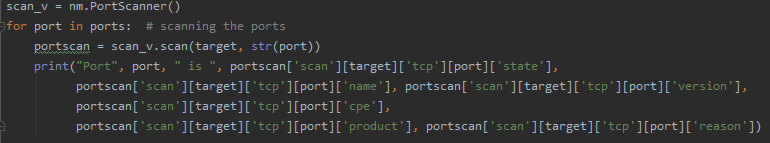


Port scanning:

Target variable have the ip address of the site and the we use if else as we have two options, we can either enter the single or number of ports or we can give the range of ports. And that ports will be append in the list and the ports will be print.

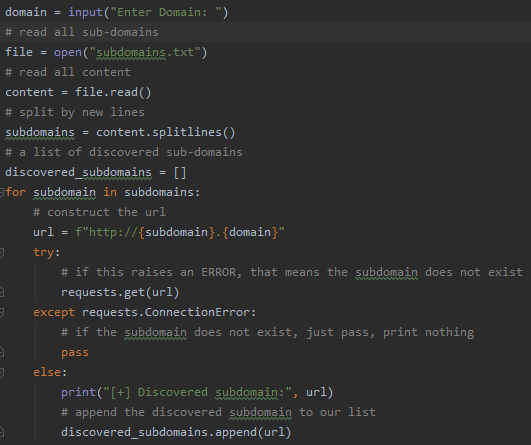


By using the nmap module we use the port scanner function of the nmap module and scanning the ports and getting the response like port, port name , port number, product, services running on the port, version of the services, cpe, reason of scan.



Subdomains:

Finding the subdomains of the site. We open a file subdomain.txt which is available on GitHub and the request will match the subdomains from that txt file



The discovered sub domains will be stored in the file and the printed on the screen

